

REMARKS:

In the outstanding Office Action, claims 1-18 and 24-26 were rejected. Claims 1-4 have been amended for clarification. New claim 27 has been added, and claims 19-23 stand cancelled. Thus, claims 1-18 and 24-27 are pending and under consideration. No new matter has been added. The rejections are traversed below.

REJECTION UNDER 35 U.S.C. §103(a):

In the outstanding Office Action, claims 1-18 and 24-26 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,754,652 ('652) and U.S. Patent No. 5,163,097 ('097).

'652 discusses a method for sequentially encrypting digits of a personal identification number (PIN) according to which a user individually encrypts a digit of the PIN by performing a function on a generated random number.

'097 discusses a method for providing secure access to a limited access system where a user uses a non-machine generated access code formed by using a selected algorithm, a password, and a dynamic variable to access the limited access system.

The present invention discloses a device and method for checking user identification where a user enters a value in response to at least one randomly or arbitrarily generated number and the user entered value is checked against a check value, resulting from the application of a user-specific formula to the at least one randomly generated number.

The Examiner compares the '652 method for individually encrypting each digit of a PIN assigned to a user with the present invention. In '652, a random single digit integer that is different for each transaction is generated and displayed for every digit of the PIN assigned to a user, which the user is prompted to sequentially add to each digit of the PIN (see, column 4, lines 59-60 of '652). The user must add the respectively generated integer displayed to each digit of the user's PIN until application of the addition function to every digit of the PIN is complete (see, abstract, lines 5-8 of '652). This means that the '652 system displays a separate integer for each of the digits of the PIN and requires the user to individually perform a function by applying the displayed integer to each digit of the PIN that the user has memorized. Accordingly, security is undermined because of the key touch information entered by the user and the integer displayed to the user.

The present invention calculates “a check value by applying a user-specific formula to at least one randomly generated number” (see, claims 6, 11 and 24-26 of the present invention). Unlike the ‘652 method that is directed to applying a check method to each digit of the PIN by generating a different integer for the same, a check value of the present invention is calculated “by applying a user-specific formula to at least one randomly generated number”. This means that the at least one randomly generated number is applied to the entire user-specific formula to provide the check value. Accordingly, the present invention only requires that the user remember the arithmetic formula, thereby eliminating the burden of memorizing various information. The ‘652 system does not teach or suggest “applying a user-specific formula to at least one randomly generated number” because it is directed to applying a generated integer to each digit of the PIN.

Amended independent claims 1 and 4 recite, “a user-defined arithmetic formula... defining calculation of variables that are assigned to respective digit positions arranged on a display screen” and display of “random digits at the respective digit positions arranged on the display screen when a user logs in”. This allows a user to be authenticated based on a comparison of “a value... calculated by assigning the random digits to said arithmetic formula” and comparing “the value with an identification-purpose number” entered by the user (see, claims 1 and 4 of the present application).

The Examiner acknowledges that the ‘652 system fails to disclose a user-specific formula including one or more elements which are either an operand or an operator where all of the elements are predetermined user-specific information except for the randomly generated number, thus relies on ‘097 as disclosing the same. In ‘097, the cipher information employed by a user includes a unique access key memorized by the user (such as a PIN), account identification (such as a bank account), and a selected cipher algorithm memorized by the user (see, column 4, lines 9-15 of ‘097). The ‘097 system explicitly states that each cipher algorithm requires that at least a user’s access key and one or more dynamic variables serve as cipher keys to generate an access code, using which the user gains access to a secure system (see, column 4, lines 31-34 and column 5, lines 26-29 of ‘097). This means that the user is required to memorize or remember the unique access key and the selected algorithm, thereby burdening the user.

It is improper to combine references where the references teach away from their combination. In re Grasselli, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). The Applicants respectfully point out that the present invention, which includes applying “a user-

specific formula to at least one randomly generated number”, and allows a user to gain access by entering a value using memorized user-specific formula in response to at least one randomly generated number, is not suggested or taught by the combination of the ‘652 and ‘097 systems discussing individual application of a function to each digit of a PIN (‘652) and expressly requiring a user to memorize an algorithm and an access key (‘097).

Accordingly, the Applicants respectfully assert that the Examiner has not met the burden of establishing a prima facie case of obviousness because the combination of the ‘652 and ‘097 systems results in a system for sequentially encrypting digits of PIN by adding a generated random number to each digits of the PIN, and gaining access using a non-machine generated access code formed by using a selected algorithm, an access key, and a dynamic variable.

It is submitted that independent claims 1, 4, 6, 11 and 24-26 are patentably distinguishable over the combination of the ‘652 and ‘097, thus withdrawal of the outstanding rejections is requested.

For at least the above-mentioned reasons, claims depending from independent claims 1, 4, 6, 11 and 24-26 are patentably distinguishable over the combination of the ‘652 and ‘097 methods. For example, as recited in claim 5, the device for checking user identification includes a registration/updating unit which “updates one of the user-specific formulas in the control-data unit with a user-entered formula only if the user entering the user-entered formula proves knowledge of said one of the user-specific formulas by entering said one of the user-specific formulas”. The ‘097 method discusses providing additional security by allowing the user the option of selecting a new cipher algorithm from the cipher algorithm pool after each transaction (see, column 6, lines 1-6 of ‘097). This means that, because the ‘097 system requires the user to input a unique access key and the selected cipher algorithm for each transaction, the update according to the ‘097 system is not accomplished until the user inputs the unique access key and the selected cipher algorithm. Thus, the ‘097 system does not teach or suggest a system that updates one of the user-specific formulas when the user proves knowledge of the user-specific formula “by entering said one of the user-specific formulas” in response to a randomly generated number(s).

Therefore, withdrawal of the rejection is respectfully requested.

NEW CLAIM:

New claim 27 has been added to further emphasize that the present invention allows a user to gain access by “prompting the user to apply a user-specific formula having at least one

operand and at least one operator to the arbitrary number" and verifying the user identification data of the user when "a calculated value generated by applying a stored user-specific formula to the arbitrary number matches a value entered by the user in response to the displaying of the arbitrary number".

This allows the present invention to provide a highly secure user identification checking method without burdening users because the user gains access using the user-specific formula without requiring the user to enter other types of identification data.

Accordingly, newly added claim 27 is patentably distinguishable from the cited reference.

CONCLUSION:

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

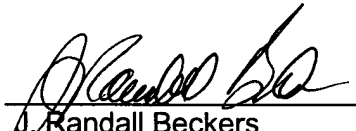
Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 10/26/4

By: 
J. Randall Beckers
Registration No. 30,358

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501